Алгебра 5
09.10.97

Теория Галуа

Часть 1. Основная теорема Теории Галуа.

Лемма. Пусть $K : L$ — расширение Галуа, и $\alpha \in K$ инвариантен относительно $G = Gal(K : L)$, т.е. $\alpha \in K^G$. Тогда $\alpha \in L$.

Доказательство: Если это не так, то $L(\alpha) \neq L$. Пусть $Q(x)$ — минимальный многочлен α, и пусть β — другой корень Q в K. Тогда $L(\alpha) \simeq L[x]/(Q) \simeq L(\beta)$. По лемме о продолжении изоморфизма, $L(\alpha) \xrightarrow{\sim} L(\beta)$ можно продолжить до автоморфизма поля K, т.е. до элемента группы Галуа, не сохраняющего α. Противоречие.

Основная Теорема. Пусть $K : L$ — расширение Галуа с группой Галуа G. Имеется взаимно-однозначное соответствие между промежуточными полями $L \subset M \subset K$ и подгруппами $H \subset G$ такое, что

1. $H \mapsto M = \phi(H) := K^H$
2. $M \mapsto H = \psi(M) := \{ h \in G \mid h(m) = m \ \forall m \in M \}$
3. $[M : L] = \frac{\sharp G}{\sharp H}$; $[K : M] = \sharp H$
4. Расширение $M : L$ нормально тогда и только тогда, когда соответствующая подгруппа $H \subset G$ нормальна.

Доказательство: Надо проверить, что $\psi(\phi(H)) = H$. Если это неверно, то пусть $M = \phi(H)$, $\psi(M) = H' \neq H$. Во всяком случае, очевидно, $H' \supset H$. Имеем $Gal(K : M) = H'$, и значит, $\sharp Gal(K : M) > \sharp H$. По теореме о примитивном элементе $K = L(\theta) = M(\theta)$. Положим $P(x) = \prod_{h \in H}(x - h(\theta))$. Коэффициентами $P(x)$ являются элементарные симметрические функции всех $h(\theta)$. Под действием элементов H корни $h(\theta)$ переставляются, а их симметрические функции остаются неизменны. По лемме получаем $P(x) \in M[x]$. Но так как θ порождает все K, мы заключаем, что $Gal(K : M) \leqslant \deg P(x) = \sharp H$. Противоречие.

Итак, $\psi(\phi(H)) = H$. Поэтому ϕ является инъекцией и сюръекцией, а значит, и биекцией. Свойство 3 очевидно, а свойство 4 следует из того, что если промежуточное поле $L \subset M \subset K$ нормально над L, то все автоморфизмы K сохраняют M (не поэлементно, а как множество). $\square$

Следствие. Правильный семнадцатиугольник можно построить циркулем и линейкой.

Доказательство: $Gal(\mathbb{Q}(\sqrt[17]{1}) : \mathbb{Q}) = \mathbb{Z}/16\mathbb{Z}$. Последовательности подгрупп $\mathbb{Z}/16\mathbb{Z} \supset \mathbb{Z}/8\mathbb{Z} \supset \mathbb{Z}/4\mathbb{Z} \supset \mathbb{Z}/2\mathbb{Z} \supset \{e\}$ отвечает последовательность расширений $\mathbb{Q} \subset K_2 \subset K_4 \subset K_8 \subset \mathbb{Q}(\sqrt[17]{1})$, каждое из которых квадратично над предыдущим. Значит, $\mathbb{Q}(\sqrt[17]{1})$ поликвадратично, то есть строится циркулем и линейкой.

Часть 2. Решение уравнений в радикалах.

Определение. Группа G называется разрешимой, если существует последовательность подгрупп $G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_n = \{e\}$ такая, что

a) G_{i+1} является нормальной подгруппой в G_i;

b) Факторгруппа G_i/G_{i+1} является циклической.

Примеры. $\mathfrak{S}_n \supset \mathfrak{A}_n$ обозначают, соответственно, группу всех подстановок n элементов и группу четных подстановок n элементов.

a) $\mathfrak{S}_3$ разрешима: $\mathfrak{S}_3 \overset{\mathbb{Z}/2\mathbb{Z}}{\supset} \mathfrak{A}_3 \overset{\mathbb{Z}/3\mathbb{Z}}{\supset} \{e\}$;

b) $\mathfrak{S}_4$ разрешима: $\mathfrak{S}_4 \overset{\mathbb{Z}/2\mathbb{Z}}{\supset} \mathfrak{A}_4 \overset{\mathbb{Z}/3\mathbb{Z}}{\supset} \mathfrak{K}_4 \overset{\mathbb{Z}/2\mathbb{Z}}{\supset} \mathbb{Z}/2\mathbb{Z} \supset \{e\}$; здесь $\mathfrak{K}_4 = \{(12)(34), (13)(24), (14)(23), e\}$ — четверная группа Кляйна.

c) $\mathfrak{S}_n$, $n \geqslant 5$, неразрешима, так как единственная нормальная подгруппа в ней — это $\mathfrak{A}_n$, которая, в свою очередь, вообще не имеет нормальных подгрупп. Мы это еще проверим в будущих лекциях.

Свойства. Если G разрешима и H — подгруппа в G, то H тоже разрешима. Если же $H \subset G$ — нормальная подгруппа, то факторгруппа G/H тоже разрешима. Абелева группа разрешима.

До конца лекции для простоты мы будем предполагать, что все поля имеют характеристику 0.

Лемма. Пусть поле L содержит все $\sqrt[n]{1}$, и $K = L(\sqrt[n]{a})$. Тогда $Gal(K : L)$ циклична.

Доказательство: Пусть θ — корень уравнения $\theta^n = a$, и $\zeta \in L$ — примитивный $\sqrt[n]{1}$. Тогда все остальные корни этого уравнения имеют вид $\zeta^k\theta$, и любая подстановка из группы Галуа имеет вид $\theta \mapsto \zeta^k\theta$, $1 \leqslant k \leqslant n$. Поэтому группа Галуа изоморфна некоторой подгруппе циклической группы корней n-ой степени из 1. $\square$

Теорема. Пусть поле L содержит все $\sqrt[n]{1}$, и $K : L$ — расширение Галуа с циклической группой Галуа $\mathbb{Z}/n\mathbb{Z}$. Тогда $K = L(\sqrt[n]{a})$.

Доказательство: Пусть σ — образующая $Gal(K : L)$, и $\zeta \in L$ — примитивный $\sqrt[n]{1}$. Для $\alpha \in K$ определим резольвенту Лагранжа: $R(\alpha) := \alpha + \zeta\sigma\alpha + \zeta^2\sigma^2\alpha + \ldots + \zeta^{n-1}\sigma^{n-1}\alpha$. Мы потом докажем, что найдется α такое, что $R(\alpha) \neq 0$. А сейчас выберем такое α и заметим, что с очевидностью $\sigma^k(R(\alpha)) = \zeta^{-k}R(\alpha)$. Поэтому $\sigma(R(\alpha)^n) = R(\alpha)^n \Rightarrow a := R(\alpha)^n \in L$, т.е. $R(\alpha) = \sqrt[n]{a}$. Более того, так как $R(\alpha) \neq 0$, этот элемент не сохраняется никаким автоморфизмом из группы Галуа кроме тождественного. По основной теореме Галуа $K = L(R(\alpha)) = L(\sqrt[n]{a})$. $\square$

Осталось доказать, что $R(\alpha) \not\equiv 0$. Для этого заметим, что Id$=$ $\sigma^0, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ задают различные гомоморфизмы из мультипликативной группы $F = K^*$ в K^*. Поэтому достаточно доказать следующую Лемму о линейной независимости гомоморфизмов:

Лемма. Пусть $c_1, \ldots, c_n$ — различные гомоморфизмы из группы F в мультипликативную группу K^*. Тогда они линейно независимы над K, т.е. если $\gamma_1 c_1(f) + \ldots + \gamma_n c_n(f) \equiv 0$, то $\gamma_1 = \ldots = \gamma_n = 0$.

Доказательство индукцией по n. База $n = 1$ очевидна. Пусть теперь для любого $f \in F$ имеем

$$\gamma_1 c_1(f) + \ldots + \gamma_n c_n(f) = 0$$

Возьмем $a \in F$ и заменим f на af. Получим

$$\gamma_1 c_1(af) + \ldots + \gamma_n c_n(af) = \gamma_1 c_1(a) c_1(f) + \ldots + \gamma_n c_n(a) c_n(f) = 0$$

Умножим предпоследнее равенство на $c_1(a)$ и вычтем из последнего. Получим

$$\gamma_2(c_2(a) - c_1(a))c_2(f) + \ldots + \gamma_n(c_n(a) - c_1(a))c_n(f) = 0$$

По предположению индукции $\gamma_2(c_2(a) - c_1(a)) = \ldots = \gamma_n(c_n(a) - c_1(a)) = 0$. Так как все c_k различны, можно выбрать a так, чтобы $c_k(a) \neq c_1(a)$, и заключить, что $\gamma_2 = \ldots = \gamma_n = 0$. $\square$

Теорема. Пусть $P(x) \in L[x]$ — неразложимый многочлен; $K : L$ — его минимальное поле разложения. Если некоторый корень $\alpha \in K$, $P(\alpha) = 0$, выражается в радикалах, то $\mathrm{Gal}(K : L)$ разрешима.

Доказательство: Присоединим перво-наперво к L корни из 1 всех степеней, которые встречаются в радикалах в выражении α. Теперь будем присоединять в соответствии с этим выражением все корни многочленов вида $x^n - a$. Каждое расширение будет нормально с циклической группой Галуа, следовательно, группа Галуа окончательного большого расширения $M \supset L$ будет разрешима. Так как M нормально и содержит α, оно содержит и все поле K. А стало быть, $Gal(K : L)$ будет разрешимой как факторгруппа $Gal(M : L)$.

Кстати, обратное утверждение тоже верно: оно немедленно следует из теоремы о расширениях с циклической группой. $\square$